BUILDING AN EFFECTIVE CYBERSECURITY PROGRAM

INSTRUCTOR COURSE DELIVERY

COURSE OUTLINE

1st Semester

1	2	3	4	5
Standardized Cybersecurity Program Design	Designing a Cybersecurity Program	Cybersecurity Frameworks & Models	Cybersecurity Technologies – Part A	Cybersecurity Technologies – Part B
Architect role and cybersecurity program roadmap	Design and development	ISO 27001/27002, NIST CSF, etc.	Countermeasures and safeguards	Countermeasures and safeguards

COURSE OUTLINE - CONTINUED

1st Semester

6

Cybersecurity Technologies – Part C

Countermeasures and safeguards

7

Training & Program Maturity

Security awareness, culture and training

8

Program Governance & Policies

Policy development and management

2nd Semester

9

Threat Management & Intelligence Gathering

Threat identification

10

Attack Surface & Vulnerability Management

Penetration testing and red teaming

2nd Semester

11

Risk Management

Risk management lifecycle

12

Incident Response & Operations Integration

Automated incident response

13

Defense-in-Depth

Layered information and asset protection

14

Security Program Testing

Penetration testing, tabletop exercise and simulations

15

Service Management

ITIL® and ITSM adoption and management

COURSE OUTLINE - CONTINUED

2nd Semester

16

Program Management Disciplines

Program management

COURSE OUTLINE - CONTINUED

LESSON 1: STANDARDIZED CYBERSECURITY PROGRAM DESIGN

WEEK 1 LESSON PLAN:
STANDARDIZED CYBERSECURITY PROGRAM DESIGN

We will cover these topics:

- Course introduction
- Today's cybersecurity threats
- Cybersecurity program drivers
- Role of the cybersecurity architect
- Roadmap
- Emerging cybersecurity technologies

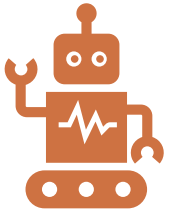
LESSON 1 LEARNING OBJECTIVES

- Understand course organization, assignments, testing and grading emphasize.
- Gain an appreciation for the types of threats a cybersecurity program should be designed to defend.
- Understand the drivers and benefits of creating a standards-based cybersecurity program.
- Understand the role and responsibilities of a cybersecurity program architect.
- Gain familiarization with the phases of creating a cybersecurity program.
- Understand how cybersecurity technology is evolving.

LECTURE: COURSE INTRODUCTION

- A study of cybersecurity principles, practices, frameworks, standards, and best practices necessary to design, build and manage a cybersecurity program.
  - Chief Information Security Officer's (CISO) perspective.
  - Roadmap of the phases required to create a comprehensive cybersecurity program.
  - Overview of the most critical information and asset protection technologies and controls.
  - Application of the most current approaches in cybersecurity architecture and design.
  - Papers, case studies and labs to reinforce learning supporting practical applications.

LECTURE: CYBERSECURITY THREATS



IoT Vulnerability Exploitation

Wireless & RF Protocol Compromise

Ransomware Attack

Supply Chain Compromise

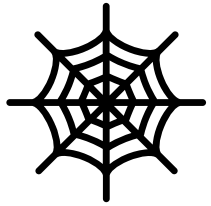
Poor Enterprise Hygiene

Cyber Warfare

Social Engineering Attacks

Business Email Compromise

Credential Stuffing



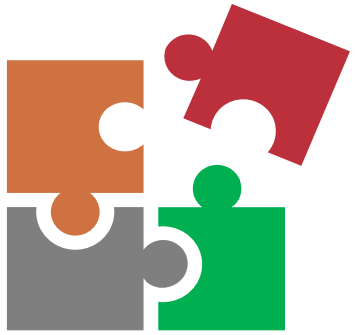
Web Application Attacks

Cloud Data Leaks

LECTURE: CYBERSECURITY PROGRAM DRIVERS

- Organizational culture.
- Critical business processes.
- Industry parameters.
- Legal and regulatory statutes.
- Operational risk profile.
- Investment appetite.
- Maturity state.

LECTURE: CYBERSECURITY ARCHITECT ROLE

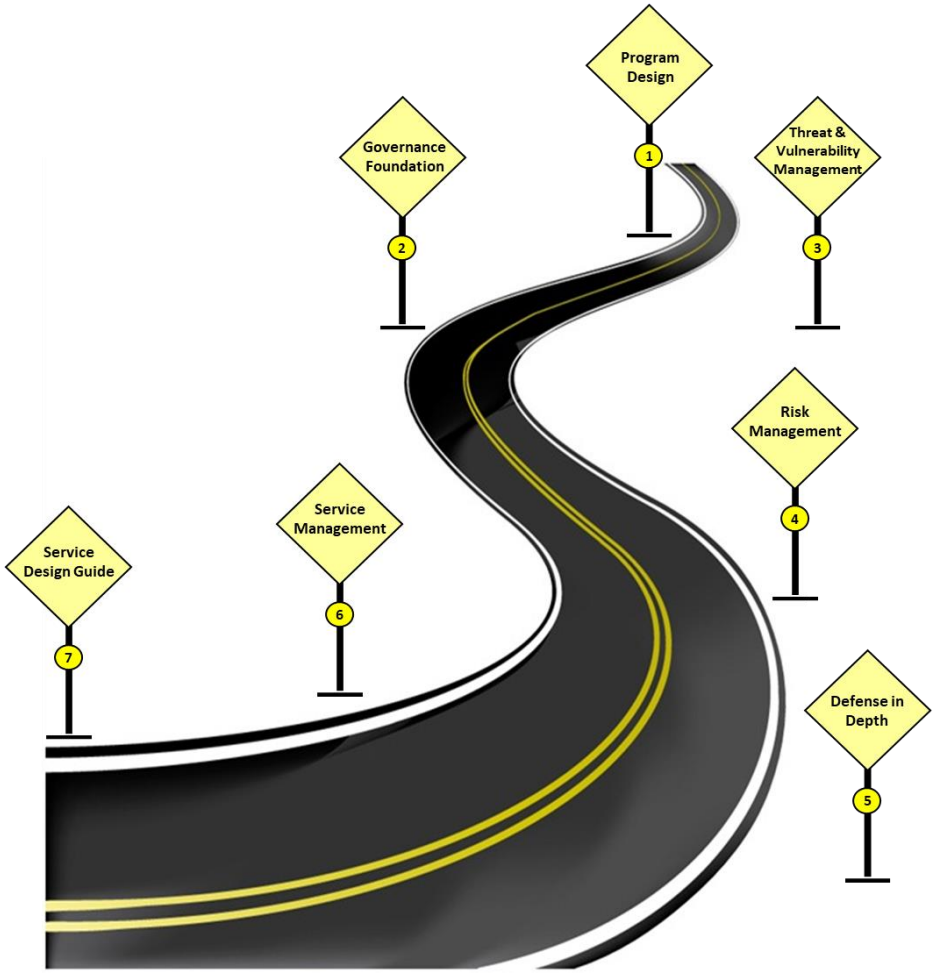


- Possess a thorough understanding of an organization's business model and technology.
- Researches, plans and designs an approach to protect information and assets.
- Defines the need for countermeasures based on an organization's risk profile.
- Keeps abreast of evolving threat and vulnerabilities in contrast to risk treatment approaches.
- Evaluates the maturity of a cybersecurity program through continuous improvement measures.

LECTURE: CYBERSECURITY ARCHITECT RESPONSIBILITIES

- Leverage cybersecurity standards, frameworks and models to create an enterprise-class security program.
- Design, build and oversee the implementation of security systems to protect critical business processes.
- Research and communicate current and emerging security threats.
- Design security architecture components to mitigate organizational risk.
- Identify security design gaps and mitigate though the design improvements, key or compensating controls.

LECTURE: CYBERSECURITY PROGRAM ROADMAP



1. Designing a Cybersecurity Program.
2. Establishing a Foundation of Governance.
3. Building a Threat, Vulnerability Detection and Intelligence Capability.
4. Building a Cyber Risk Management Capability.
5. Implementing a Defense-in-Depth Strategy.
6. Applying Service Management to Cybersecurity Programs.
7. Cybersecurity Program Design Toolkit.

LECTURE: DESIGNING A CYBERSECURITY PROGRAM

- Define a cybersecurity program's end state.
- Define the program's general structure and supporting components.
- Understand available cybersecurity frameworks.
- Understand the core technologies required to protect information and assets.

LECTURE: ESTABLISH A FOUNDATION OF GOVERNANCE

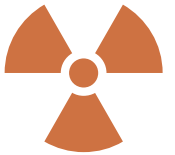
- Understand the parameters of governance.
- Adopt program design principles.
- Understand available governance frameworks and models.
- Learn about strategies to automate governance programs.
- Understand how to raise program maturity.

LECTURE: BUILDING A THREAT,VULNERABILITY DETECTION AND INTELLIGENCE CAPABILITY

- Learn how to classify organization assets and information.
- Identify threats and vulnerabilities.
- Identify attack vectors.
- Create an attack surface.
- Learn how to acquire and apply threat intelligence.

LECTURE: BUILDING A CYBER RISK MANAGEMENT CAPABILITY

- Create a risk profile.
- Understand risk frameworks and models.
- Know how to calculate risk.
- Understand risk treatment approaches.
- Manage risk.

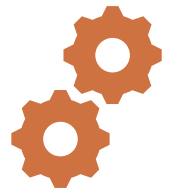


LECTURE: IMPLEMENTING A DEFENSE-IN-DEPTH STRATEGY

- Define a defensive strategy to protect information and assets.
- Build a cybersecurity service catalog.
- Define controls for:
  - Governance, risk and compliance
  - Application, database and software security
  - Threat and vulnerability management
  - Security operations (SecOps)
  - Device and data protection
  - Cloud service and infrastructure protection

LECTURE: APPLYING SERVICE MANAGEMENT TO CYBERSECURITY PROGRAMS

- Implement orchestration and automation functionality.
- Integrate service management practices.
- Ensure controls function properly.
- Deploy resiliency and continuity in cybersecurity program.



LECTURE: EMERGING CYBERSECURITY TECHNOLOGIES

1. Artificial intelligence
2. Augmented reality (AR)
3. Blockchain
4. Deep learning
5. Hardware-based authentication
6. Quantum computing encryption
7. Machine learning (ML)
8. Photonics data transfer

LESSON 1 ASSIGNMENTS

- **Reading:** Chapter 1- Designing a Cybersecurity Program.
- **Paper:** Research and write a 2- to 4-page paper on what you believe are the top-10 cybersecurity threats facing organizations today. Include graphics, tables and sources to illustrate your conclusions.
- **Lab:** Pair up in teams to discuss and document essential drivers of developing a cybersecurity program for either a FinServ, healthcare, manufacturing or retail organization.

END OF LESSON 1